

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-044353

(43)Date of publication of application : 14.02.1997

(51)Int.Cl.	G06F	9/06
	G06F	9/06
	G06F	15/00
	G09C	1/00
	G09C	1/00

(21)Application number : 07-194695

(22)Date of filing : 31.07.1995

(71)Applicant : TOSHIBA CORP

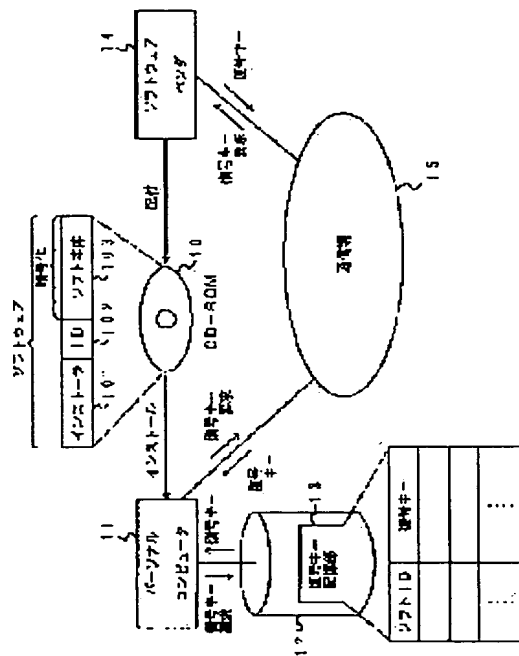
(72)Inventor : YOSHIDA HIDEKI
SEGAWA HIDEO
IMAI TORU

(54) DECODING KEY MANAGEMENT METHOD, COMPUTER ADOPTING THE METHOD, AND SOFTWARE METHOD AND SYSTEM USING THE KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the reliability of a software distribution system using a cipher by increasing the number of degrees of freedom of erasing and re-installation of ciphered software.

SOLUTION: A decoding key to decode a ciphered software main body 103 is preserved in a decoding key storage part 13 correspondingly to the software ID. An installer 101 retrieves the decoding key storage part 13; and if the pertinent decoding key is not found, the decoding key is obtained from a software vendor 104 by communication with this vendor 104. After this decoding key is stored in the decoding key storage part 13 corresponding to the software ID, the software main body 103 is decoded and is installed to a hard disk device 12. Since the key is reused at the time of decoding the software main body 103 again, it is unnecessary for a user to get the decoding key from the vendor 14 plural times.



LEGAL STATUS

[Date of request for examination]

14.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3507594

[Date of registration]

26.12.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

“ decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

【特許請求の範囲】

【請求項1】 暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入すると共に、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存し、
前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とするソフトウェア復号鍵管理方法。

【請求項2】 暗号化された複数のソフトウェアをインストール可能なコンピュータであって、
ソフトウェア識別情報とそのソフトウェアを解読するための復号鍵とを対応付けて格納するための復号鍵記憶手段と、
導入対象の暗号化されたソフトウェアからソフトウェア識別情報を取得し、そのソフトウェア識別情報を利用して、前記暗号化されたソフトウェアを解読するための復号鍵を前記復号鍵記憶手段から検索する復号鍵検索手段と、
この復号鍵検索手段によって前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入する手段と、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から前記ソフトウェアに対応する復号鍵を通信網を介して入手するための通信手続きを実行する復号鍵入手手段と、
この復号鍵入手手段によって入手された復号鍵を、前記導入対象の暗号化されたソフトウェアを特定するための識別情報と対応付けて前記復号鍵記憶手段に保存する手段と、
前記入手された復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入する手段とを具備することを特徴とするコンピュータ。

【請求項3】 少なくとも1つの暗号化されたソフトウェア本体と、復号鍵を利用して前記ソフトウェア本体を復号化するための復号化プログラムとを含むソフトウェアを、記録媒体または通信媒体を介して流通させるソフトウェア流通方法であって、
前記復号化プログラムを、前記ソフトウェア本体を導入

すべきコンピュータに実行させることによって、
前記コンピュータの記憶装置内から前記ソフトウェア本体を解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存することを特徴とするソフトウェア流通方法。

【請求項4】 暗号化されたソフトウェアを配布し、使用料の支払いと引き替えに前記暗号化されたソフトウェアを復号化するための復号鍵を発行するソフトウェア流通方法で使用される記録媒体であって、
この記録媒体には、少なくとも1つの暗号化されたソフトウェア本体と、復号鍵を利用して前記ソフトウェア本体を復号化するための復号化プログラムとが含まれ、
前記復号化プログラムには、暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存する手続きが記述されていることを特徴とする記録媒体。

【請求項5】 暗号化されてユーザに配布されるソフトウェアそれぞれを解読するための復号鍵を保持する計算機センタと、この計算機センタから復号鍵を入手してソフトウェアを復号化するユーザ端末とを接続可能な通信網を利用して、ソフトウェアを流通させるソフトウェア流通システムにおいて、
前記ユーザ端末は、
ソフトウェア識別情報とそのソフトウェアを解読するための復号鍵とを対応付けて格納するための復号鍵記憶手段と、
導入対象の暗号化されたソフトウェアを解読するための復号鍵を、前記復号鍵記憶手段から検索する復号鍵検索手段と、
この復号鍵検索手段によって前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェ

アを復号化して前記ユーザ端末に導入する手段と、
前記復号鍵を検索できなかったとき、前記計算機センタに復号鍵を要求する事によって、前記ソフトウェアに対応する復号鍵を前記計算機センタから通信網を介して入手する復号鍵入手手段と、

この復号鍵入手手段によって入手された復号鍵を、前記導入対象の暗号化されたソフトウェアを特定するための識別情報と対応付けて前記復号鍵記憶手段に保存する手段と、

前記入手された復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記ユーザ端末に導入する手段とを具備し、

前記計算機センタは、

前記ユーザ端末からの復号鍵要求に応答して、ソフトウェア使用量を課金するための情報を生成する手段と、
前記復号鍵要求に応答して、復号鍵をユーザ端末に送信する手段とを具備することを特徴とするソフトウェア流通システム。

【請求項 6】 暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、

前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、

前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から前記ソフトウェアに対応する復号鍵を入手し、その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、

前記ソフトウェアを前記コンピュータの記憶装置から消去するとき、前記復号鍵を前記記憶装置に保存し、

前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とするソフトウェア復号鍵管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化されたソフトウェアを復号化するための鍵（キー）の管理方法およびその方法が適用されるコンピュータ、並びに復号鍵を使用したソフトウェア流通方法および流通システムに関する。

【0002】

【従来の技術】従来、コンピュータで使用されるソフトウェアは、それぞれ個別にフロッピーディスクなどの記憶媒体に格納され、マニュアルなどともにパッケージに封入された状態で小売店で販売されるのが通常の販売形態であった。

【0003】このようなパッケージソフトウェアの場合、ソフトウェアの利用許諾などを行なうライセンス

グは、ソフトウェアのパッケージの販売と不可分の形で行なわれるのが一般的である。たとえば、パッケージを開封した時点でソフトウェアの利用契約が成立する旨が記述された文書がソフトウェアに付随して配布される場合や、パッケージに付属の利用者登録書をただちに記入してベンダと利用契約を結ぶことが求められる場合が多い。

【0004】これに対し、最近では、従来のようにソフトウェアを個別に販売する形式でのライセンスングではなく、より自由な流通形態とソフトウェア権利者保護を目的とした新たな流通方法が提案されている。このような流通方法の典型的な例としては、文献（森亮一、田代秀一「ソフトウェア・サービス・システム（ＳＳＳ）の提案」電子情報通信学会論文誌「87/1 Vol. J70-D No. 1」）が知られている。

【0005】この文献には、“ソフトウェアサービスシステム（ＳＳＳ）”と称されるソフトウェア流通システムが紹介されている。ＳＳＳでは、暗号化されたソフトウェア本体とそれを解読するための機能を持つヘッダ部とから構成されるソフトウェア構造が利用される。また、“共通クレジット”と“許諾条件プログラム”という２つの概念を利用して、ユーザとソフトウェア権利者間のライセンスングとソフトウェア使用料の管理が行われている。

【0006】“共通クレジット”は、量的にどれだけのソフトウェアの使用をユーザに許すかという情報が記憶されたＩＣカードなどから構成されるものである。ＳＳＳによって配布されたソフトウェアを使用したいと考えるユーザは、まず、ＳＳＳのサービスセンタに行って適当な料金を支払い、その額に対応する情報が書き込まれた共通クレジットを受け取る。

【0007】“許諾条件プログラム”は、共通クレジットに書き込まれた情報の値からユーザの契約残高を認識し、ソフトウェアを実行を許可または禁止するためのプログラムである。この許諾条件プログラムは、ある値以上の共通クレジットが計算機上に存在することを確認した上でソフトウェアが実行を許し、そしてそのソフトウェアの価値に応じた量だけ共通クレジットの値（契約残高に相当する）をデクリメントする。

【0008】しかしながら、このような共通クレジットを使用したソフトウェア使用料の管理方法では、共通クレジットの複製やそのデータ書き替えに対する保護が必要とされ、そのために、例えば共通クレジットのリード／ライトを制限するための専用のハードウェア機構などが必要となるという問題がある。

【0009】

【発明が解決しようとする課題】そこで、最近では、暗号化されたソフトウェアをユーザに無償または低価格で配布しておき、ユーザが使用を希望するソフトウェアを復号化するためのキーを使用料と引き換えにユーザに発

行するというソフトウェア流通システムが提案され始めている。

【0010】このような流通システムを採用することによって、ソフトウェアベンダは個別のソフトウェアのパッケージ作成および流通にかかるコストを節約できるほか、暗号化されたソフトウェアの内容を紹介するためのデモンストレーション版をCD-ROMなどの媒体と一緒にパッケージングしておくことにより、その媒体をソフトウェアの有効な宣伝手段として用いることができる。また、ユーザから見ると、ソフトウェアの正式な購入前にそのソフトウェアが購入に値するかどうかを試用によって確認できるという利点がある。

【0011】ユーザは、希望するソフトウェアの使用料の支払いと引き換えに復号キーを受け取り、その受け取ったキーを使って自分の計算機のハードディスクにソフトウェアの正式版をインストールする。

【0012】このように、復号キーを利用したソフトウェア流通システムは、その復号キーの受け渡しによってソフトウェア使用料の管理を行えるため、SSSのような共通クレジットやそれを管理するための専用のハードウェアが不要となり、より自由度の高い流通形態を実現できる。

【0013】ところで、ユーザによるコンピュータの通常の使用形態を考えると、ハードディスクの空き容量を増やすためにインストール済みのソフトウェアを一旦消去し、後日必要になった時に再インストールするということが頻繁に行われている。暗号化されていない通常のパッケージソフトウェアの場合には、パッケージに含まれている記録媒体自体はユーザの手元に残っているので、ハードディスク上にインストールされたソフトウェア自体は消えてしまっても構わない。後日そのソフトウェアが必要になった場合は、あらためて記録媒体からのインストールが可能だからである。

【0014】これに対して、前述したような復号キーを利用したソフトウェア流通システムの場合には、ユーザの手元に残っているの実行可能なソフトウェアは、復号キーを利用して復号化されたハードディスク上のソフトウェアだけである。したがって、もしユーザがソフトウェアベンダから利用料と引き替えに入手した復号キーを紛失した場合、そのソフトウェアを再インストールする場合には、同じソフトウェアの使用料を再び支払って復号キーを入手しなければならない。このことは、暗号化を利用したソフトウェア流通システムの信頼性を低下させ、その流通システムの普及を妨げる要因となる。

【0015】この発明はこのような点に鑑みてなされたものであり、暗号化を利用したソフトウェア流通システムにおけるキー管理を改善して、一旦正当な手順で復号化されたソフトウェアについてはソフトウェアベンダからキーを入手しなくても再インストールできるようにし、ソフトウェアの消去および再インストールを自由に

行う事が可能な復号鍵管理方法を提供することを目的とする。

【0016】

【課題を解決するための手段】この発明による復号鍵管理方法は、暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入すると共に、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存し、前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とする。

【0017】この復号鍵管理方法においては、ソフトウェアの配布元から復号鍵を入手したとき、その復号鍵は、ソフトウェア本体の復号化に利用されると共に、例えば、復号化されたソフトウェア本体と別個のファイルなどとしてコンピュータの記憶装置内に保存される。したがって、復号化されたソフトウェア本体を記憶装置から消去した場合でも、復号鍵は保存されたまま消去されない。したがって、初めてインストールするソフトウェアについてはソフトウェア配布元から復号鍵を入手する手続きが必要となるが、既にインストールされたことのあるソフトウェアを再インストールする場合には記憶装置に保存されている復号鍵によって復号化することができる。よって、一旦正当な手順で復号化されたソフトウェアについてはソフトウェアベンダからキーを入手しなくてもその再インストールを実行できるようになり、ソフトウェアの消去および再インストールを自由に行う事が可能になる。

【0018】ソフトウェア本体がインストールされる記憶装置と復号鍵が保存される記憶装置は例えば同一のハードディスク装置などであってもよいが、ソフトウェア本体がインストールされる記憶装置とは別に、復号鍵を記憶するための復号鍵記憶装置を用意しても良い。この場合、復号鍵記憶装置には消去されたソフトウェアに対応する復号鍵だけが保存されていれば十分であり、記憶装置に残っているソフトウェアの復号鍵は不要ある。このため、ソフトウェアの配布元から復号鍵を入手したときは、復号鍵はソフトウェア本体がインストールされる記憶装置に格納しておき、そのソフトウェア本体が消去されるときに、そのソフトウェア本体に対応する復号鍵を復号鍵記憶装置に移して保存することが好ましい。

【0019】また、この発明によるソフトウェアインス

トールの手順は、暗号化ソフトウェアと付随して配布される復号化プログラムに記述しておくことが好ましい。この場合、インストールに必要な全ての手続きが復号化プログラムによって自動的に実行されるので、ユーザは、初めてインストールするものか、再インストールするものかによらず、使用したいソフトウェア内の復号化プログラムを実行するだけで済む。

【0020】また、このような復号化プログラムは、配布されるソフトウェア単位ではなく、各種暗号化ソフトウェアをコンピュータにインストールするための共通の10 インストーラとして実現してもよい。この場合、ソフトウェア配布元から入手された復号鍵は、ソフトウェア識別情報と対応付けて保存する事が好ましい。これにより、ソフトウェア識別情報を検索キーとして利用できるようになり、どの暗号化ソフトウェアをインストールする場合でも、それに対応する復号鍵の検索処理を行うことが可能になる。

【0021】

【発明の実施の形態】以下、図面を参照して、この発明の実施の形態を説明する。図1には、この発明の一実施形態に係るソフトウェア流通システム全体の構成が示されている。

【0022】このソフトウェア流通システムは、暗号化されたソフトウェアをユーザに無償または低価格で配布しておき、ソフトウェア使用料の支払いと引き換えにユーザが使用を希望するソフトウェアを復号化するための復号キーを発行するというソフトウェア流通方法を実現するためのものであり、複数の加入ユーザ端末とソフトウェアベンダ、およびそれらを繋ぐ通信網から構成される。ここで、暗号化されたソフトウェアとは、暗号化された30 プログラム、暗号化されたデータなどを意味する。

【0023】図1においては、加入ユーザ端末としてパーソナルコンピュータ11が代表して示されており、そのパーソナルコンピュータ11は、電話回線やISDNなどの通信網15を介してソフトウェアベンダ14に設置された計算機センタに接続されている。

【0024】ソフトウェアベンダ14は、暗号化された複数のソフトウェアと、それらソフトウェアの内容を紹介するためのデモンストレーション版ソフトなどが一緒に収容されたCD-ROM10などの大容量記録媒体を通じて、無償または低価格でユーザに配布する。また、ソフトウェアベンダ14は、配布した暗号化ソフトウェアそれぞれについて、それを復号化するための復号キーを保持および管理している。

【0025】CD-ROM10に記録された1つのソフトウェアは、インストーラ101、ソフトウェア識別情報(ID)102、およびソフトウェア本体103から構成されている。この場合、ソフトウェア本体103は暗号化されているが、インストーラ101およびソフトウェア識別情報(ID)102については暗号化はされ

ていない。また、デモンストレーション版についても、暗号化はなされていない。

【0026】インストーラ101は、暗号化されたソフトウェア本体103を復号化してユーザの使用するパーソナルコンピュータ11にインストールするためのプログラムである。ソフトウェア識別情報(ID)102は、暗号化されたソフトウェアを特定するための固有のIDである。ソフトウェア本体103は、所定のオペレーティングシステム下で動作するアプリケーションプログラムやユーティリティプログラム、あるいは画像情報などの各種データファイルなどである。

【0027】パーソナルコンピュータ11の2次記憶装置として使用されるハードディスク装置12には、パーソナルコンピュータ11で実行されるオペレーティングシステムや各種アプリケーションプログラム、または各種データファイルがインストールされている。また、このハードディスク装置12の記憶領域には、復号キー記憶部13が用意されている。

【0028】復号キー記憶部13は、インストーラ101によって参照可能な独立した1種のデータファイルであり、一度インストールされた暗号化ソフトウェアそれぞれについてそのソフトウェアIDと、そのソフトウェアを復号化するためにソフトウェアベンダ14から入手した復号キーとが対応付けられて保存されている。この復号キー記憶部13の復号キーは、再インストールされる暗号化ソフトウェアを復号化するために利用される。

【0029】復号キー記憶部13へのソフトウェアIDおよび復号キーの保存は、ソフトウェアベンダ14から復号キーを入手したときに行われる。また、実際には、復号キー記憶部13には消去されたソフトウェアに対応する復号鍵だけが保存されていれば十分であるので、ソフトウェア本体103がが消去されるときに、それに対応するソフトウェアIDおよび復号キーを復号キー記憶部13に保存しても良い。

【0030】図2には、インストーラ101のプログラム構造が示されている。インストーラ101は、図2に示されているように、復号キー検索プログラム、通信プログラム、復号およびインストールプログラム、および復号キー保存プログラムを含んでいる。以下、これらプログラムによって実行される機能を図3を参照して説明する。

【0031】復号キー検索プログラムは、復号キー記憶部13を検索して、暗号化されたソフトウェア本体103を復号化するための復号キーを取得する。前述したように、復号キー記憶部13には、既にインストールされた暗号化ソフトウェアに対応するソフトウェアIDと復号キーとが登録されている。このため、復号キー検索プログラムによる復号キー検索は、ソフトウェア識別情報(ID)102と復号キー記憶部13のソフトウェアIDとを順次比較する順次検索、あるいは2分検索などに

よって行われる。

【0032】通信プログラムは、ソフトウェア使用料の支払いとの引き換えにソフトウェアベンダ14から復号キーを入手するために、通信回線15を介してソフトウェアベンダ14と通信する。この通信プログラムには、復号キー要求メッセージをソフトウェアベンダ14に送信するルーチンと、ソフトウェアベンダ14から復号キーを受信するルーチンが含まれている。この通信プログラムは、復号キー検索プログラムによる復号キー検索が失敗した時、つまり該当する復号キーが復号キー記憶部13に存在しなかったときに実行される。

【0033】復号およびインストールプログラムは、復号キー検索プログラムによるキー検索が成功した場合にはそのキーを、失敗した場合には通信プログラムによってソフトウェアベンダ14から入手されたキーを使用して、ソフトウェア本体103を復号化し、ハードディスク装置12にインストールする。

【0034】復号キー保存プログラムは、通信プログラムによってソフトウェアベンダ14から入手された復号キーを、ソフトウェアIDと対応付けて復号キー記憶部13に保存する。

【0035】このように構造を持つインストーラ101によれば、ソフトウェアベンダ14から復号キーを入手したときに、その復号キーは、ソフトウェア本体103の復号化に利用されると共に、その復号化されたソフトウェア本体103とは別個のファイルとして復号キー記憶部13に保存される。このため、復号化されたソフトウェア本体をハードディスク装置12から消去しても復号キーについては消去されずに復号キー記憶部13に保存されたまま維持される。

【0036】したがって、既にインストールされたことのあるソフトウェアを再インストールする場合には、復号キー記憶部13に保存されている復号キーを利用することによりそれを直ちに復号化することができる。また、初めてインストールする暗号化ソフトウェアについては、インストーラ101によって自動的にベンダ14から復号キーを入手することができる。

【0037】次に、図4を参照して、通信プログラムによってソフトウェアベンダ14に送信される復号キー要求メッセージのデータ構造について説明する。復号キー要求メッセージには、図示のように、通信に必要な情報を含むヘッダ部21に加え、パーソナルコンピュータ11のマシンID22、インストール対象の暗号化ソフトウェアのソフトウェアID23、ユーザ名24、およびユーザのクレジット番号などが含まれている。

【0038】次に、図5を参照して、復号キー要求メッセージを受信した場合におけるソフトウェアベンダ14の動作を説明する。ソフトウェアベンダ14は、復号キー要求メッセージからソフトウェアIDを検出し、ユーザが希望しているソフトウェアを特定する。そして、そ

のソフトウェアに対応する使用料金、ユーザ名、クレジット番号などから課金処理のために必要な情報を生成し、自らまたはクレジット会社などに委託して課金処理を行う。この後、ソフトウェアベンダ14は、ソフトウェアIDに対応する復号キーを、復号キー要求メッセージ発行元のユーザに送信する。この場合、復号キーはユーザのマシンIDを用いて暗号化して送り、インストーラ201がそれをマシンIDを用いて復号化してから使用するという運用形態を利用する事もできる。

【0039】このように、復号化キーの要求および発行によってソフトウェア使用料の管理が自動的に行われる。図6には、インストーラ101の機能をパーソナルコンピュータ11に組み込んでおき、それを各種暗号化ソフトウェアをコンピュータ11にインストールするための共通のインストーラとして利用する場合の例が示されている。

【0040】すなわち、図6のパーソナルコンピュータ11には復号キー管理システム51が設けられており、この復号キー管理システム51は複数の暗号化ソフトウェアの共通インストーラとして機能として利用される。復号キー管理システム51は、この発明の流通システムを実現するために各ユーザのパーソナルコンピュータ11にインストールされて使用されるプログラムとして実現する事ができる。

【0041】この場合、復号キー管理システム51には、図2に示したインストーラ101と同様のプログラム群、すなわち、復号キー検索プログラム、通信プログラム、復号およびインストールプログラム、および復号キー保存プログラムから構成できる。

【0042】このような復号キー管理システム51を利用する場合には、暗号化ソフトウェアには、ソフトウェア本体とソフトウェアIDが登録されていれば良く、インストーラは不用である。各暗号化ソフトウェアのソフトウェアIDは、復号キー記憶部13の検索に利用される。

【0043】次に、図7乃至図9を参照して、図1のソフトウェア流通システムにおける復号キー管理処理の手順を具体的に説明する。図7には、図1のソフトウェア流通システムの運用形態の一例が示されている。ここでは、図1のハードディスク装置12に対応する記憶装置として、復号キー記憶部兼ソフトウェア本体記憶部61が使用されている。図中の破線は、ソフトウェア識別子(ID)および復号キーのみが復号キー記憶部兼ソフトウェア本体記憶部61に記憶されており、ソフトウェア本体は消去されて記憶されていない状態を表している。

【0044】ソフトウェア本体入手部62が通信回線や図1のCD-ROM10などの記憶媒体の購入などの手段によってソフトウェアベンダ14から入手した暗号化ソフトウェアをユーザのパーソナルコンピュータ11にインストールする際には、復号キー入手部63は、その

10

20

30

40

50

ソフトウェアのソフトウェアIDを検索のキーとして使用して、復号キー記憶部兼ソフトウェア本体記憶部61からそのソフトウェアの復号キーを検索する。復号キー入手部63は、前述したインストーラ101または復号キー管理システム51の復号キー検索プログラム、通信プログラム、および復号キー保存プログラムに相当している。

【0045】見つかった場合はその復号キーを利用するが、見つからなかった場合は、復号キー入手部63がソフトウェアベンダ14等から復号キーを通信回線・記憶媒体の購入などの手段によって入手し、ソフトウェアIDと復号キーを対応付けて復号キー記憶部兼ソフトウェア本体記憶部61に格納する。そして、ソフトウェア本体入手部62によってソフトウェア本体が復号化され、復号キー記憶部兼ソフトウェア本体記憶部61にインストールされる。ソフトウェア本体入手部62は、前述したインストーラ101または復号キー管理システム51の復号およびインストールプログラムに相当している。

【0046】あるソフトウェア本体を消去する際には、復号キー保存部64によってソフトウェア本体のみが消去され、ソフトウェアIDおよび復号キーはそのまま復号キー記憶部兼ソフトウェア本体記憶部61内に保存される。これは、ソフトウェアIDと復号キーとの組みをソフトウェア本体と別個に記憶しておくことなどによって実現できるものである。

【0047】また、復号キー保存部64は、ソフトウェア本体を消去するという点で、ファイル管理システムとして実現できる。この場合、復号キー保存部64は、ユーザからのプログラムファイル消去命令に応じて該当するソフトウェア本体だけを削除することになる。また、ファイル消去命令に応じて、消去対象のソフトウェア本体に対応するソフトウェアIDおよび復号キーを復号キー記憶部兼ソフトウェア本体記憶部61から読み取っておき、ソフトウェア本体の消去後に、読み取ったソフトウェアIDおよび復号キーを復号キー記憶部兼ソフトウェア本体記憶部61に書き戻すといった処理を行ってもよい。

【0048】このようにして、復号キー保存部64により、ソフトウェアIDおよび復号キーはソフトウェア本体が消去されても復号キー記憶部兼ソフトウェア本体記憶部61にそのまま維持される。

【0049】図7の復号キー記憶部兼ソフトウェア本体記憶部61では、ソフトウェア1、…、nがインストールされ、そのうちソフトウェア2、nなどのソフトウェア本体が消去されているが、ソフトウェア識別子および復号キーはそれらのソフトウェアを含めて1、…、nすべてについて保存されている。

【0050】なお、このように復号キー記憶部とソフトウェア本体記憶部と兼ねることにより、保存の処理が簡易であるほか、ハードディスクなどのソフトウェア本体

記憶部以外には他の外部記憶装置が不要であるという利点がある。

【0051】図8には、図1のソフトウェア流通システムの他の運用形態の一例が示されている。ここでは、ソフトウェア本体記憶部71は図1のハードディスク装置12に相当し、これとは別の記憶装置として復号キー記憶部75が設けられている。

【0052】ソフトウェア本体入手部72が通信回線や記憶媒体の購入などの手段によってソフトウェアベンダ14から入手した暗号化ソフトウェアをインストールする際には、まずそのソフトウェアIDを検索のキーとして復号キー入手部73が復号キー記憶部75からそのソフトウェアの復号キーを検索する。復号キー入手部73は、前述したインストーラ101または復号キー管理システム51の復号キー検索プログラム、通信プログラム、および復号キー保存プログラムに相当している。

【0053】見つかった場合はその復号キーを利用するが、見つからなかった場合は、復号キー入手部73がソフトウェアベンダ14等から復号キーを通信回線・記憶媒体の購入などの手段によって入手し、ソフトウェアIDと復号キーをソフトウェア本体記憶部71に格納する。そして、ソフトウェア本体入手部72によってソフトウェア本体が復号化され、ソフトウェア本体記憶部71にインストールされる。ソフトウェア本体入手部72は、前述したインストーラ101または復号キー管理システム51の復号およびインストールプログラムに相当している。

【0054】あるソフトウェア本体を消去する際には、復号キー保存部74によってソフトウェア識別子・復号キー・ソフトウェア本体がソフトウェア本体記憶部71から消去され、ソフトウェアIDおよび復号キーが復号キー記憶部75に保存される。すなわち、復号キー保存部74は一種のファイル管理システムでもあり、削除対象のソフトウェア本体に対応するソフトウェアIDおよび復号キーをソフトウェア本体記憶部71から取り出して、それを復号キー記憶部75に保存する。このため、復号キー記憶部75には、ソフトウェア本体記憶部71から削除されたソフトウェア本体に対応するソフトウェアIDおよび復号キーだけが保存されることになり、ソフトウェア本体記憶部71に残っているソフトウェア本体に対応するソフトウェアIDおよび復号キーについては保存されない。よって、復号キー記憶部75に不要な情報（消去されていないソフトウェア本体のソフトウェアIDおよび復号キー）が保存されることがなくなり、検索効率の向上などを図ることができる。

【0055】図8の例では、ソフトウェア本体記憶部はソフトウェア1、…、nがインストールされていたが、そのうち2、nなどのソフトウェア本体が消去されたため、それらのソフトウェアのソフトウェアIDおよび復号キーもソフトウェア本体記憶部71から消去されてい

る。これらの消去されたソフトウェアのソフトウェアIDおよび復号キーは復号キー記憶部75に格納されている。

【0056】ここでは、ソフトウェアIDおよび復号キーをソフトウェア本体とは別の記録媒体に記憶することによって、災害などによってソフトウェア本体を記録した媒体が障害を受け、ソフトウェア本体が失われた場合でも、ソフトウェアIDおよび復号キーは失われないという利点がある。

【0057】また、この媒体としてフロッピーディスクなどの取り外し可能な媒体を利用することによって、他の計算機にソフトウェアをインストールすることもできる。この場合には、前述したマシンIDによる復号キーの暗号化は行われないものとする。

【0058】図9には、暗号化ソフトウェアのインストール処理の手順が示されている。ここでは、暗号化ソフトウェアと一緒に配布されるインストーラ101を使用してインストールする場合を例にとって説明する。

【0059】ユーザによって実行が指示されると、まず、インストーラ101の復号キー検索プログラムが起動され、復号キー記憶部(図1の復号キー記憶部13、図7の復号キー記憶部兼ソフトウェア本体記憶部61、または図8の復号キー記憶部75)から該当するソフトウェア本体の復号キーを検索し、復号キー記憶部に復号キーが存在するか否かを調べる(ステップS11)。

【0060】復号キー記憶部に目的とする復号キーが存在しなかったならば、通信プログラムが実行され、復号キー入手処理が行われる(ステップS12)。すなわち、図2のようにデータ構造を持つ復号キー要求メッセージが通信回線を介してユーザのパーソナルコンピュータからソフトウェアベンダに送られ、そこで使用料支払いのための手続きが行われる。その後、復号キーが通信回線を介してソフトウェアベンダからユーザのパーソナルコンピュータに送られる。なお、ユーザのパーソナルコンピュータが通信回線に接続されてない場合には、通信プログラムは復号キーを入手する必要がある旨のメッセージやソフトウェアベンダの電話番号などを画面表示して、ユーザに対して復号キーの入手を促せばよい。

【0061】ソフトウェアベンダから入手された復号キーは、復号キー保存プログラムによってソフトウェアIDと対応付けられて復号キー記憶部(図1の復号キー記憶部13、図7の復号キー記憶部兼ソフトウェア本体記憶部61、または図8のソフトウェア本体記憶部71)に格納される(ステップS13)。

【0062】この後、入手した復号化キーによってソフトウェア本体が復号化され(ステップS14)、記憶装置(図1のハードディスク装置12、図7の復号キー記憶部兼ソフトウェア本体記憶部61、または図8のソフトウェア本体記憶部71)にインストールされる(ステップS15)。

【0063】一方、復号キー記憶部に目的とする復号キーが存在したならば、ステップS12、S13の処理は行われず、復号キー記憶部に保存されている復号キーが利用されて、ソフトウェア本体の復号化処理(ステップS14)、およびインストール処理(ステップS15)が実行される。

【0064】なお、以上の説明では、復号キーは常にソフトウェアIDと対応付けて保存するように説明したが、暗号化ソフトウェアと一緒に配布されるインストーラ101を使用してインストールする場合には、復号キーを1つのファイルとして保存し、そのファイル名としてソフトウェアIDを利用することともできる。

【0065】

【発明の効果】以上説明したように、この発明によれば、ソフトウェアの識別子とソフトウェアを復号化するためのキーとが保存され、次回にそのソフトウェア本体を再び復号化する際にはそのキーが再利用されるため、利用者は復号キーを複数回入手せずに済む。よって、ソフトウェアの消去および再インストールを自由に行う事が可能になり、暗号化を利用したソフトウェア流通システムの信頼性の向上を図ることができ、その流通システムの普及に寄与することができる。

【図面の簡単な説明】

【図1】この発明の一実施形態に係るソフトウェア流通システム全体の構成を示すブロック図。

【図2】同実施形態に係るソフトウェア流通システムで配布される暗号化ソフトウェアに付随するインストーラのプログラム構造の一例を示す図。

【図3】図2のインストーラの機能を説明するための図。

【図4】同実施形態に係るソフトウェア流通システムにおいてユーザ端末からソフトウェアベンダに送信される復号キー要求メッセージのデータ構造の一例を示す図。

【図5】同実施形態に係るソフトウェア流通システムにおけるソフトウェアベンダの機能を説明するための図。

【図6】同実施形態に係るソフトウェア流通システムのユーザ端末に設けられる復号キー管理システムの機能を説明するための図。

【図7】同実施形態に係るソフトウェア流通システムの運用形態の一例を概念的に示す図。

【図8】同実施形態に係るソフトウェア流通システムの運用形態の他の例を概念的に示す図。

【図9】同実施形態に係るソフトウェア流通システムにおける暗号化ソフトウェアのインストール手順を説明するためのフローチャート。

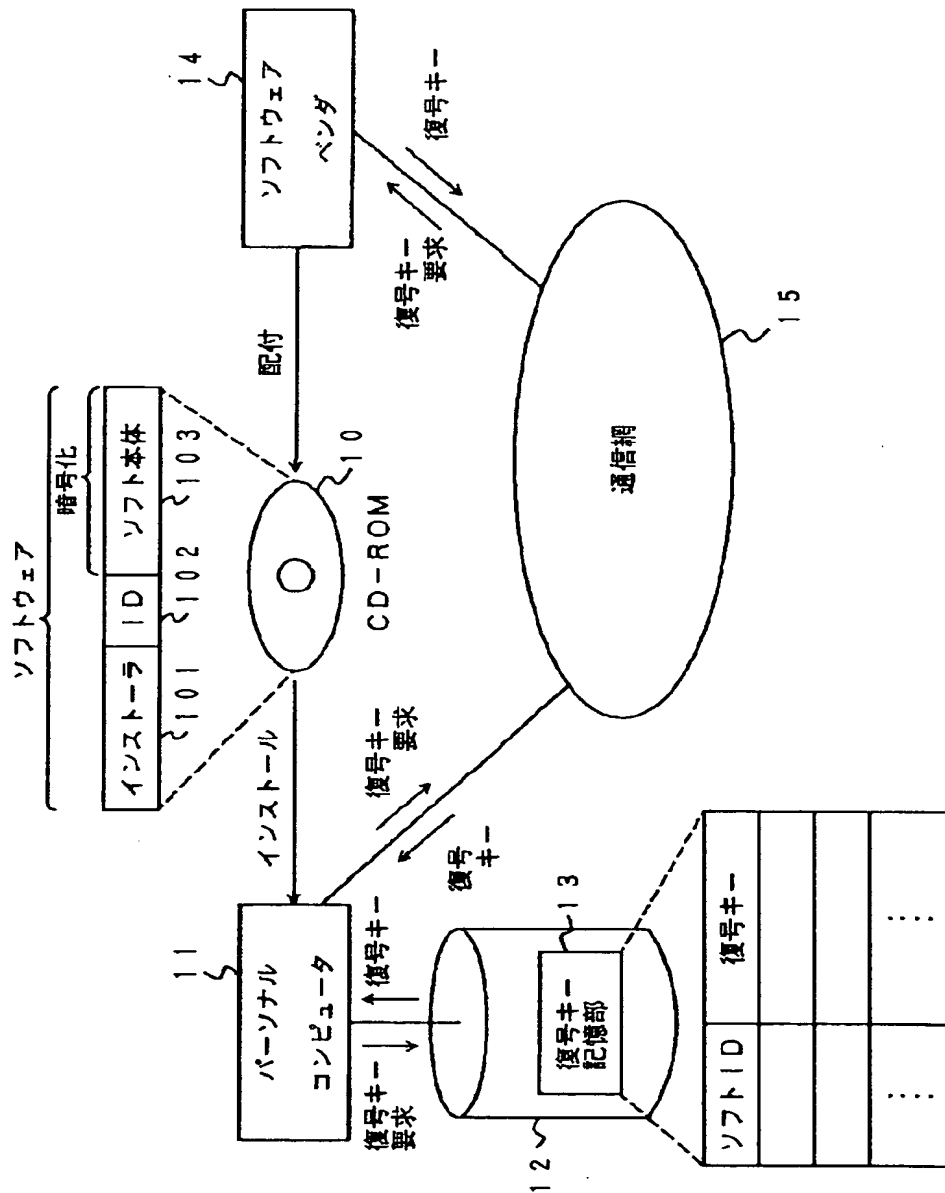
【符号の説明】

11…パーソナルコンピュータ(ユーザ端末)、12…ハードディスク装置、13、75…復号キー記憶部、14…ソフトウェアベンダ、15…通信網、51…復号キー管理システム、61…復号キー記憶部兼ソフトウェア本

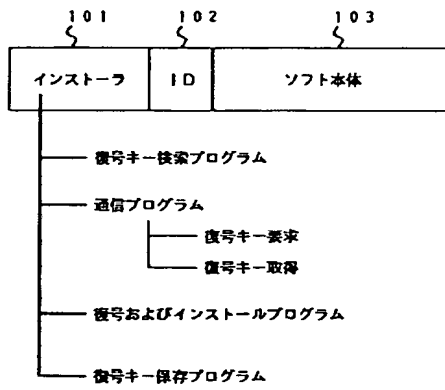
体記憶部、62、72…ソフトウェア本体入手部、63、73…復号キー入手部、64、74…復号キー保存部、71…ソフトウェア本体記憶部、101…インストール

ーラ、102…ソフトウェアID、103…ソフトウェア本体。

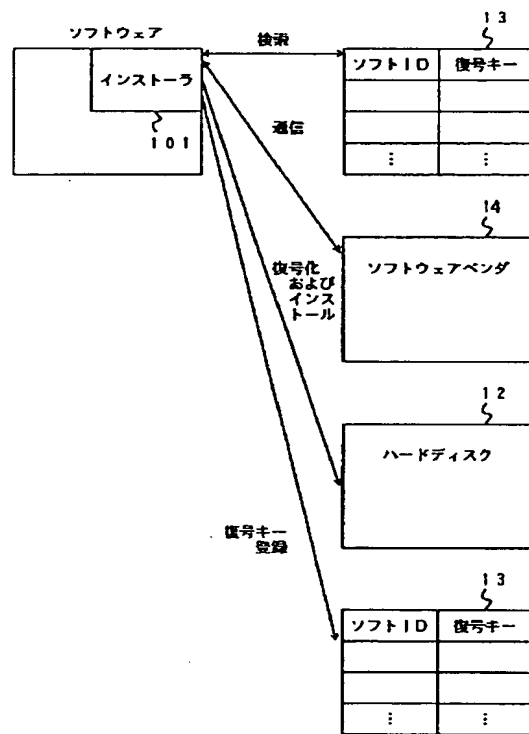
【図1】



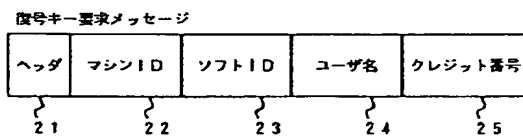
【図2】



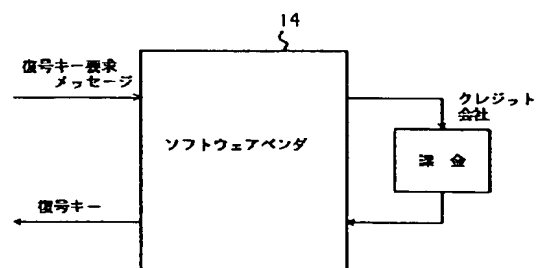
【図3】



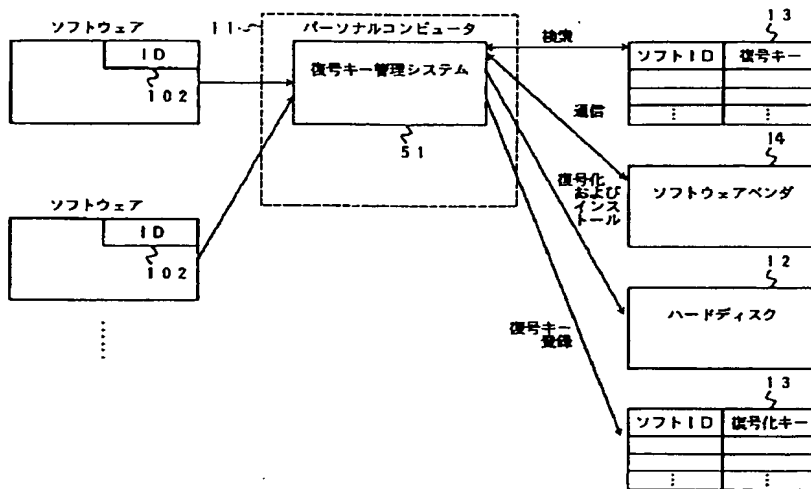
【図4】



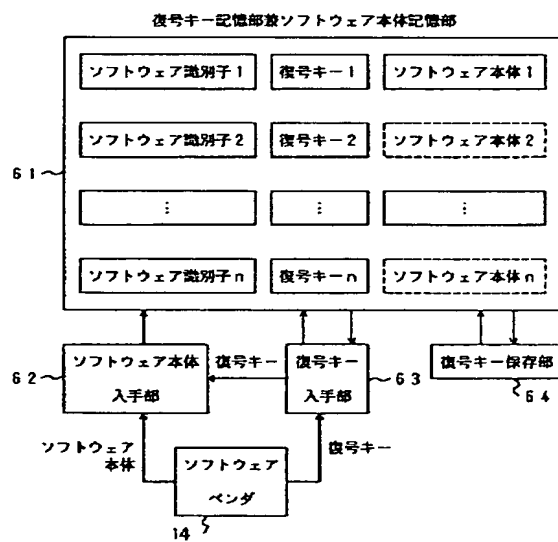
【図5】



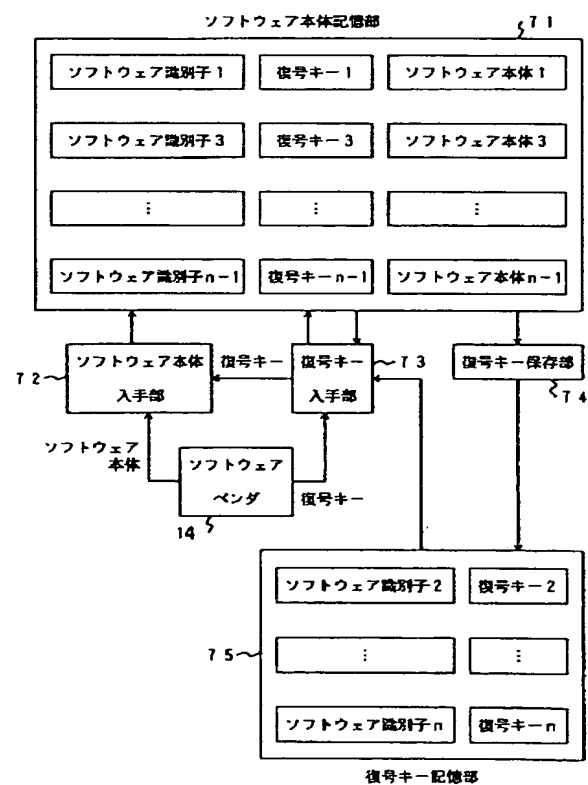
【図6】



【図7】



【図8】



【図9】

